

Overview

[WhiteSource](#) is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.

WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server. It works per project and does not offer real-time alert capabilities like the **Full platform** which is generally recommended for larger development teams, wanting to automate their open source management throughout the entire software development lifecycle (from the repositories to post-deployment stages) and across all projects and products.

What's covered in this lab

This lab shows how you can use **WhiteSource Bolt with Azure DevOps** to automatically detect alerts on vulnerable open source components, outdated libraries, and license compliance issues in your code. You will be using WebGoat, a deliberately insecure web application, maintained by OWASP designed to teach web application security lessons.

Azure DevOps integration with WhiteSource Bolt will enable you to:

1. Detect and remedy vulnerable open source components.
2. Generate comprehensive open source inventory reports per project or build.
3. Enforce open source license compliance, including dependencies' licenses.
4. Identify outdated open source libraries with recommendations to update.

Before you begin

1. Refer the [Getting Started](#) page before you follow the exercises.
2. Use [Azure DevOps Demo Generator](#) to provision the WhiteSource project on your Azure DevOps Organization.

Exercise 1: Activate WhiteSource Bolt

In your Azure DevOps Project, under **Pipelines** section, go to **White Source Bolt** tab, provide your **Work Email**, **Company Name** and click *Get Started* button to start using the *Free* version.

You're almost there...

Want to get alerts on vulnerable open source components, outdated libraries and license compliance issues in your project?
Complete this form and let's roll!

Work email

Company name

Get Started

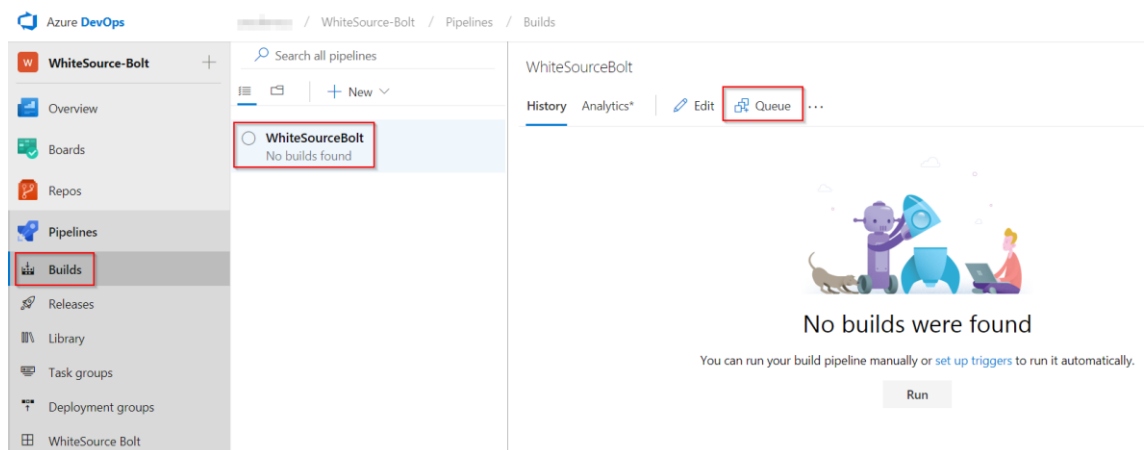
Upon activation, the below message is displayed.

✓ You are using a FREE version of WhiteSource Bolt

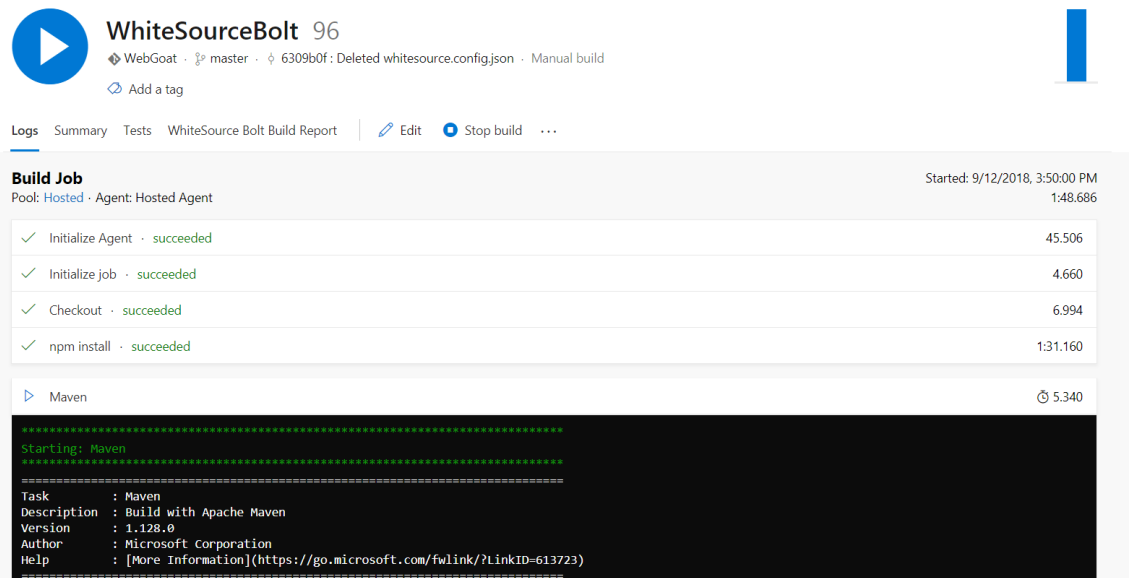
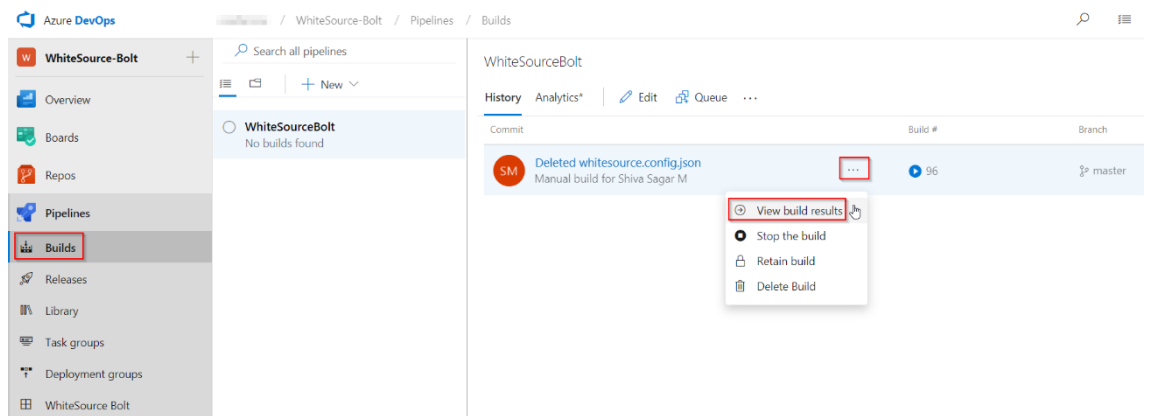
Exercise 2: Trigger a build

You have a **Java code** provisioned by the Azure DevOps demo generator. You will use **WhiteSource Bolt** extension to check the vulnerable components present in this code.




1. Go to **Builds** section under **Pipelines** tab, select the build definition **WhiteSourceBolt** and click on **Queue** to trigger a build.





2. To view the build in progress status, click on ellipsis and select **View build results**.

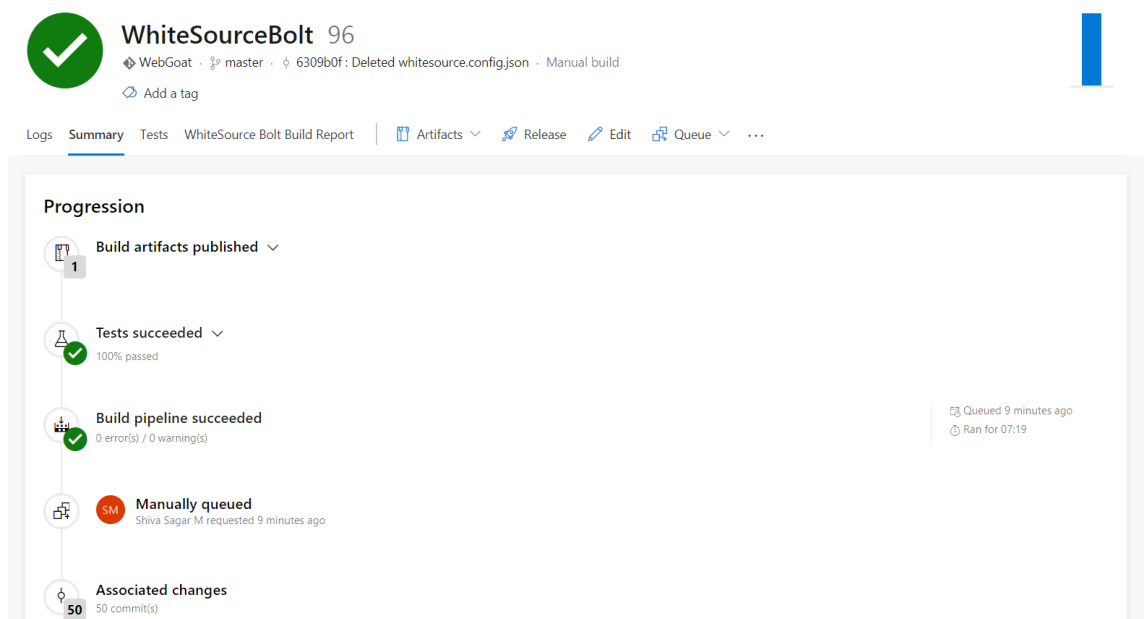


- While the build is in progress, let's explore the build definition. The tasks that are used in the build definition are listed in the table below.

Tasks	Usage
 npm	Installs and publishes npm packages required for the build
 Maven	builds Java code with the provided pom xml file
 WhiteSource Bolt	scans the code in the provided working directory/root directory to detect security vulnerabilities, problematic open source licenses

Tasks	Usage
 Copy Files	copies the resulting JAR files from the source to the destination folder using match patterns
 Publish Build Artifacts	publishes the artifacts produced by the build

- Once the build is completed, you will see the summary which shows **Test results**, **Build artifacts** etc. as shown below.



The screenshot shows the WhiteSource Bolt build summary page. At the top, there is a green checkmark icon and the text "WhiteSourceBolt 96". Below this, it says "WebGoat · master · 6309b0f: Deleted whitesource.config.json · Manual build" and "Add a tag". The page has tabs for "Logs", "Summary", "Tests", and "WhiteSource Bolt Build Report". The "Summary" tab is selected. The main content area shows a "Progression" section with a vertical timeline of build steps:

- Build artifacts published** (1 step)
- Tests succeeded** (100% passed)
- Build pipeline succeeded** (0 error(s) / 0 warning(s))
- Manually queued** (SM) (Shiva Sagar M requested 9 minutes ago)
- Associated changes** (50 commit(s))

On the right side of the "Build pipeline succeeded" step, it says "Queued 9 minutes ago" and "Ran for 07:19".

- Navigate to **White Source Bolt** tab under **Pipelines** section and wait for the report generation of the completed build to see the vulnerability report.

Exercise 3: Analyze Reports

WhiteSource bolt automatically detects OpenSource components in the software including transitive dependencies and their respective licenses.

Security Dashboard

The security dashboard shows the vulnerability of the build. This report shows the list of all vulnerable open source components with **Vulnerability Score**, **Vulnerable Libraries**, **Severity Distribution**.



You can see the opensource license distribution and a detailed view of all components and links to their metadata and licensed references.

Outdated Libraries

WhiteSource Bolt also tracks outdated libraries in the project, getting all the detailed information and links to newer versions and recommendations.

Outdated Libraries (33) [hide](#)

Library	Versions	Recommendations	Exist In Build Definitions
angular-1.4.3.js	Your version: 1.4.3, Released: Jul-20-2015 Newest stable version: 1.6.6, Released: Aug-18-2017 95 new versions since your most recent update	Consider updating to latest version	WhiteSource Bolt
angular-resource-1.4.3.js	Your version: 1.4.3, Released: Feb-17-2016 Newest stable version: 1.6.6, Released: Aug-18-2017 40 new versions since your most recent update	Consider updating to latest version	WhiteSource Bolt
angular-route-1.4.3.js	Your version: 1.4.3, Released: Jul-20-2015 Newest stable version: 1.6.6, Released: Aug-18-2017 95 new versions since your most recent update	Consider updating to latest version	WhiteSource Bolt
aopalliance-repackaged-2.4.0-b10.jar	Your version: 2.4.0-b10, Released: Feb-06-2015 Newest stable version: 2.4.0, Released: Jan-05-2016 81 new versions since your most recent update	Consider updating to latest version https://hk2.java.net/external/aopalliance-repackaged	WhiteSource Bolt
commons-codec-1.9.jar	Your version: 1.9, Released: Dec-21-2013 Newest stable version: 1.11, Released: Oct-17-2017 3 new versions since your most recent update	Consider updating to latest version http://commons.apache.org/proper/commons-codec/	WhiteSource Bolt
commons-lang3-3.1.jar	Your version: 3.1, Released: Nov-15-2011 Newest stable version: 3.4.0.redhat-2, Released: Sep-12-2017 9 new versions since your most recent update	Consider updating to latest version http://commons.apache.org/lang/	WhiteSource Bolt

Summary

With Azure DevOps and WhiteSource Bolt integration, you can *shift-left* your open source management. The integration allows you to have alerts in real time, on vulnerabilities and other issues to help you take immediate action.